

MBSE Methodology for FM System Design

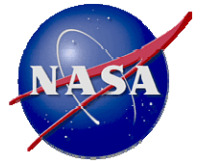
(Model Based System Engineering Methodology for Fault Management System Design)

Lui Wang, Michel Izygon*, Ph.D., Shira Okon*/ ER6
Spacecraft Software Engineering Branch, *Tietronix Software
JSC/NASA

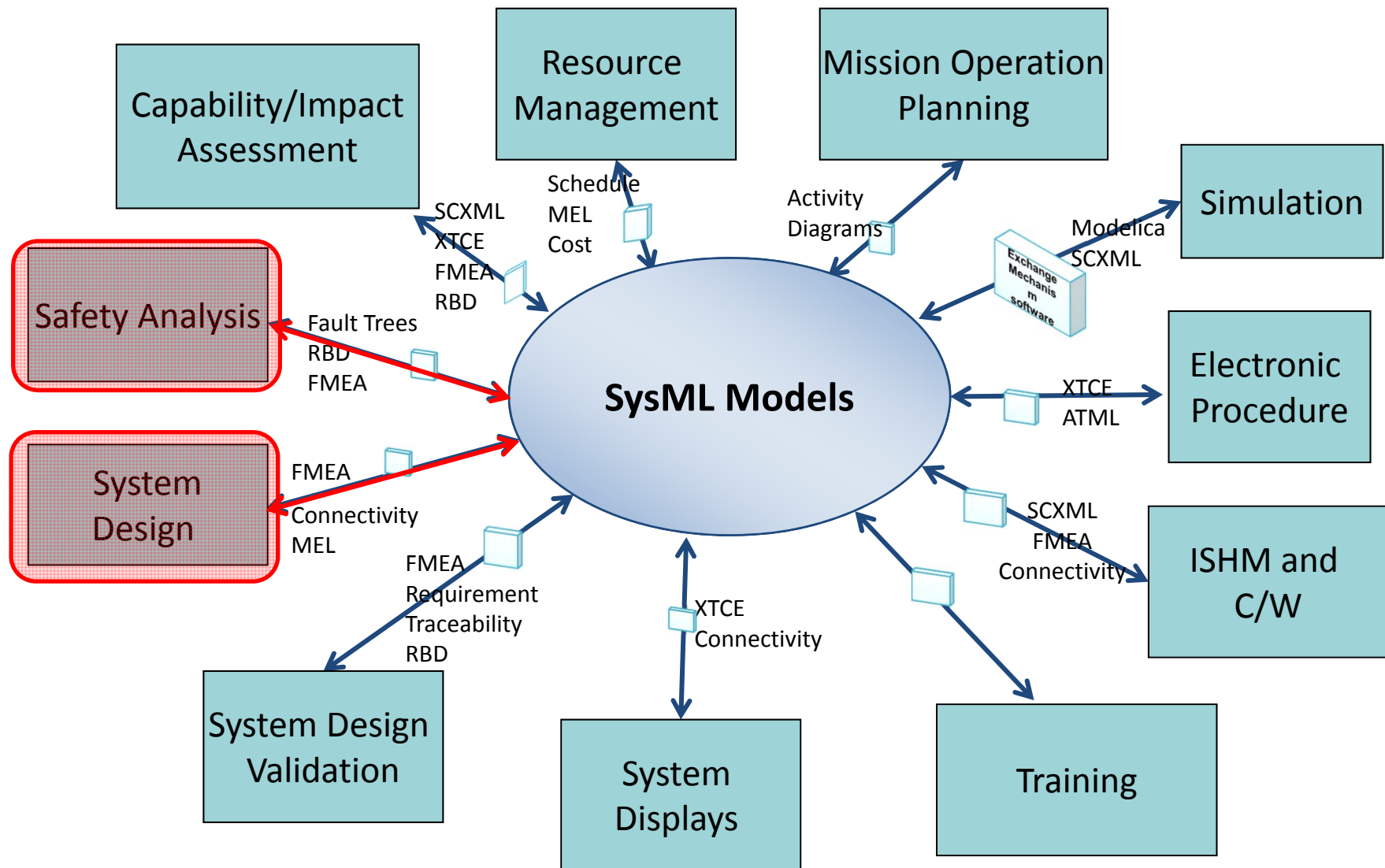
Magdy Bareh, Castet, Jean-Francois, Nunes, Jeffery, Lorraine Fesq
JPL/NASA

January 29, 2015

MBSE Context



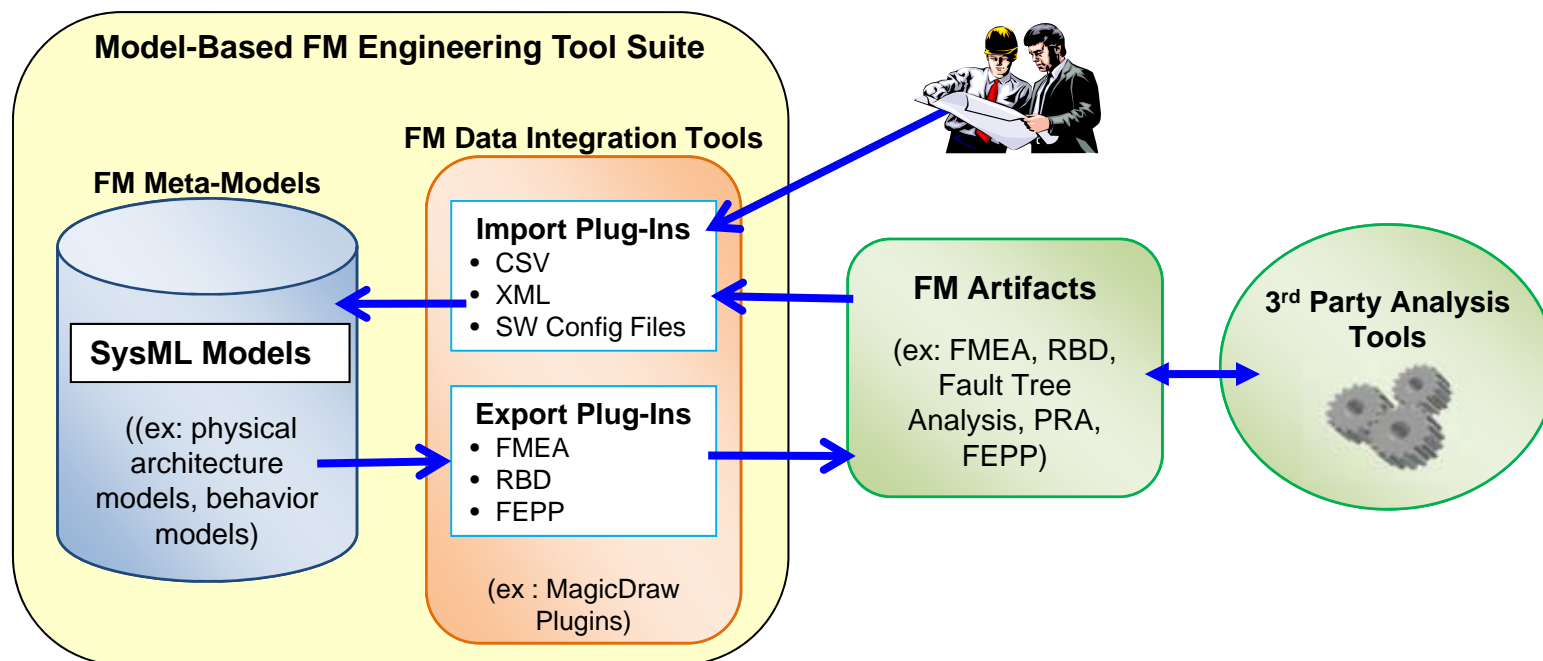
Model once and Use many times



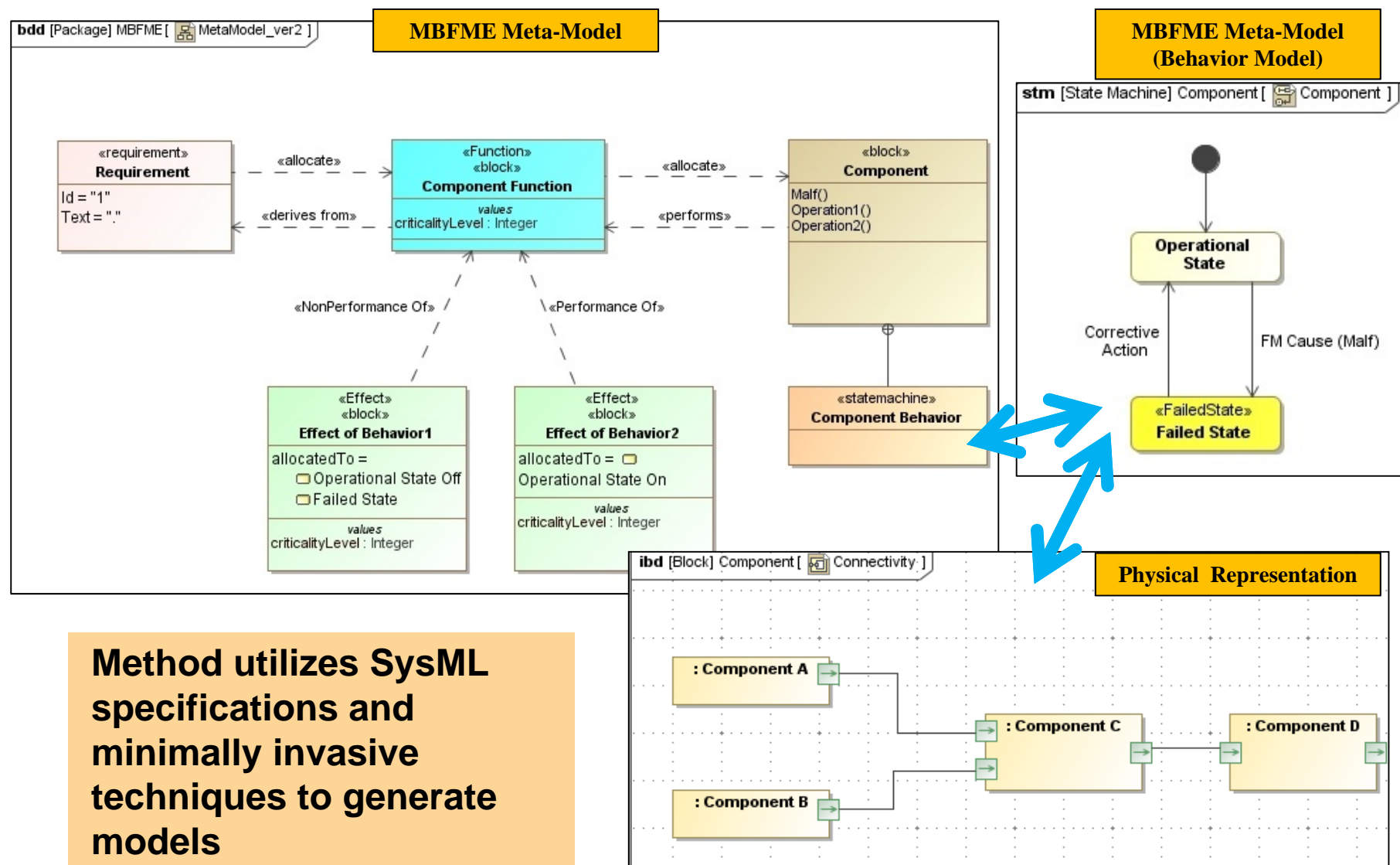


MBFME Tool Suite Concept

Model based Fault Management Engineering (MBFME)

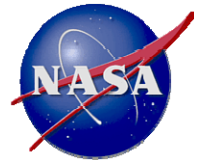


MBFME Meta-Model

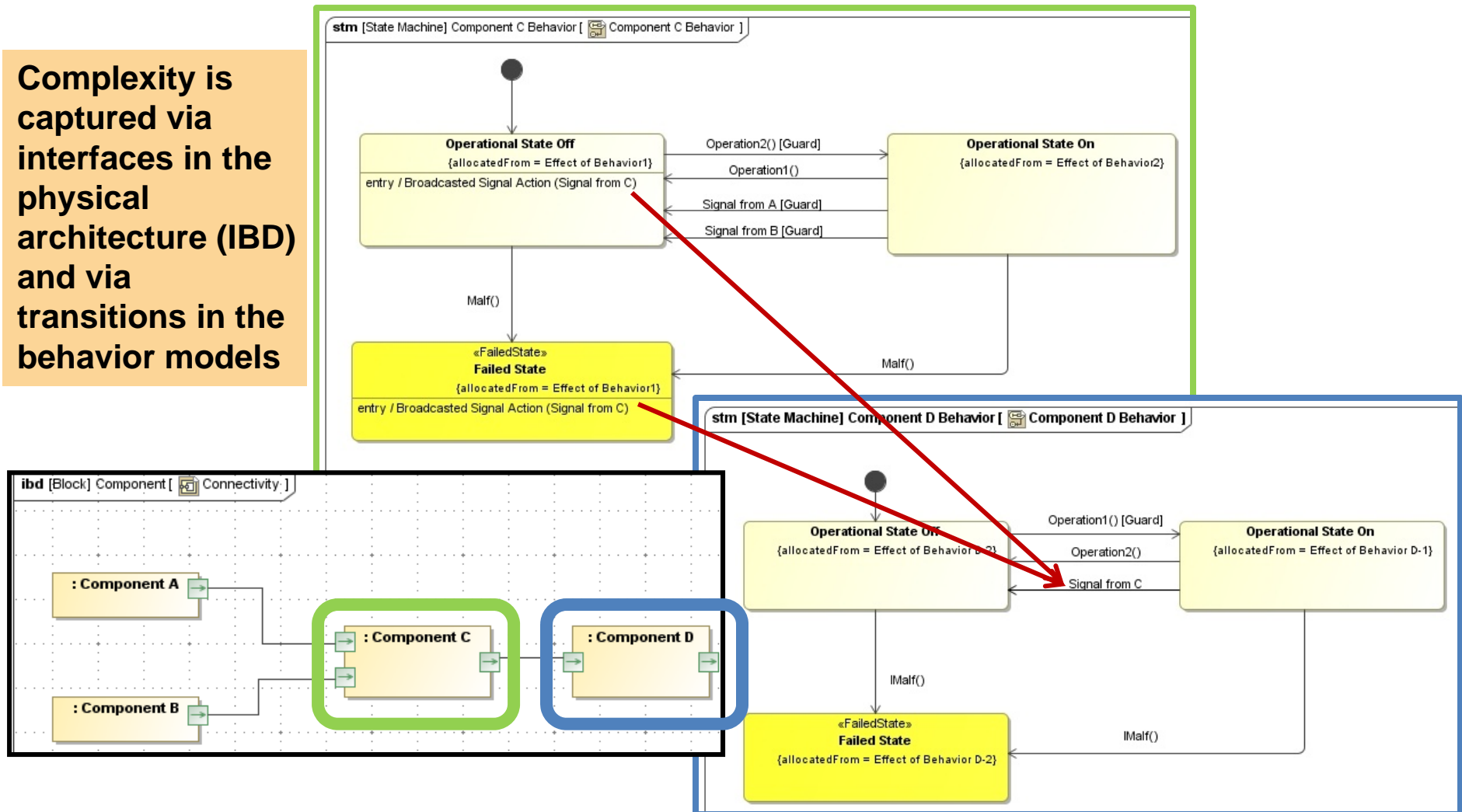


Method utilizes SysML specifications and minimally invasive techniques to generate models

MBFME Meta-Model (System Behavior)



Complexity is captured via interfaces in the physical architecture (IBD) and via transitions in the behavior models

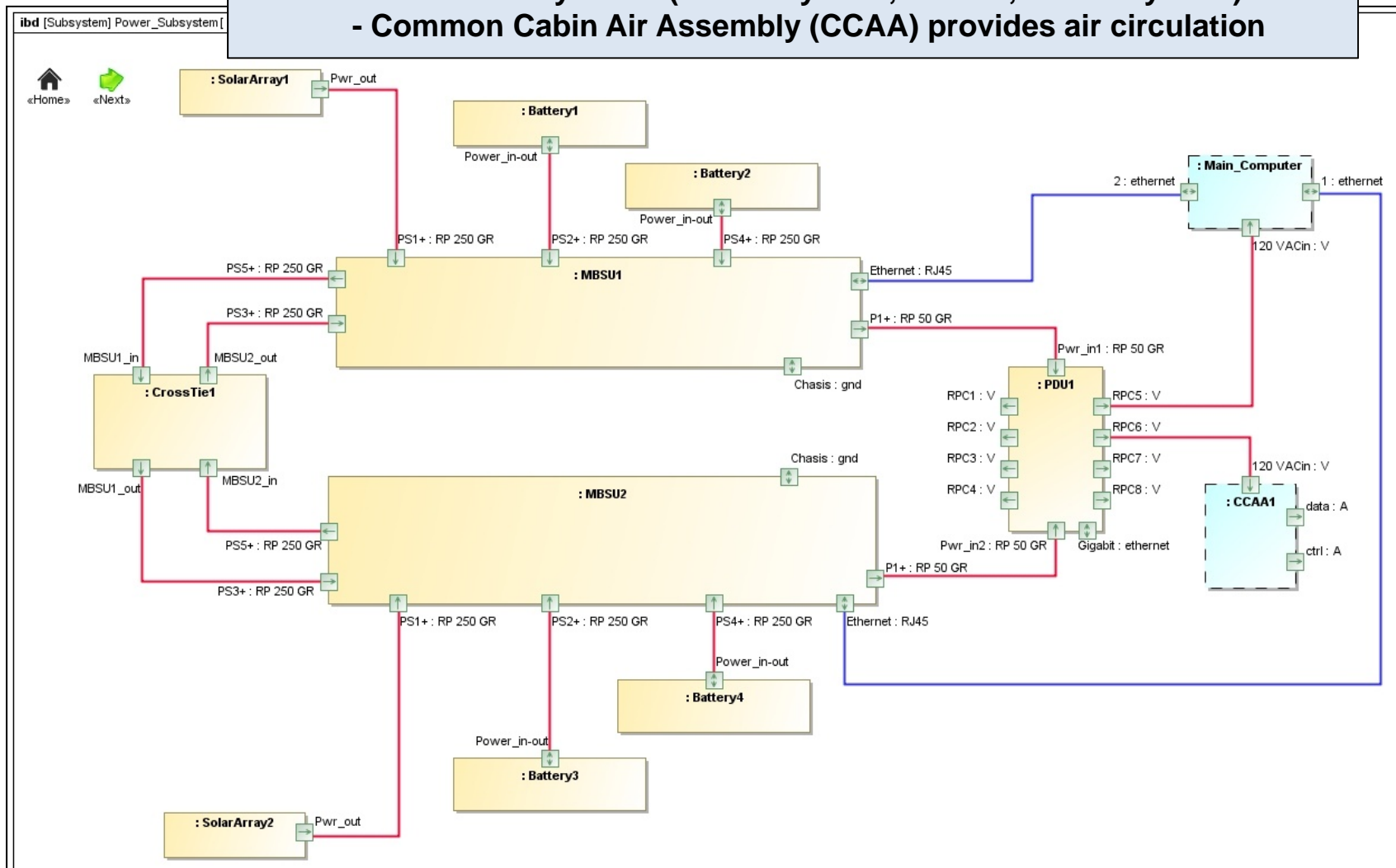


Power Subsystem Internal Block Diagram (IBD)

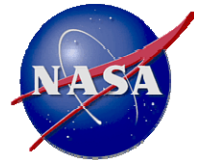


Applied MBFME Methodology to the Fan in the Can SysML model

- References a NASA spacecraft power architecture
- Contains 3 Subsystems (Power System, ECLSS, C&DH System)
 - Common Cabin Air Assembly (CCAA) provides air circulation

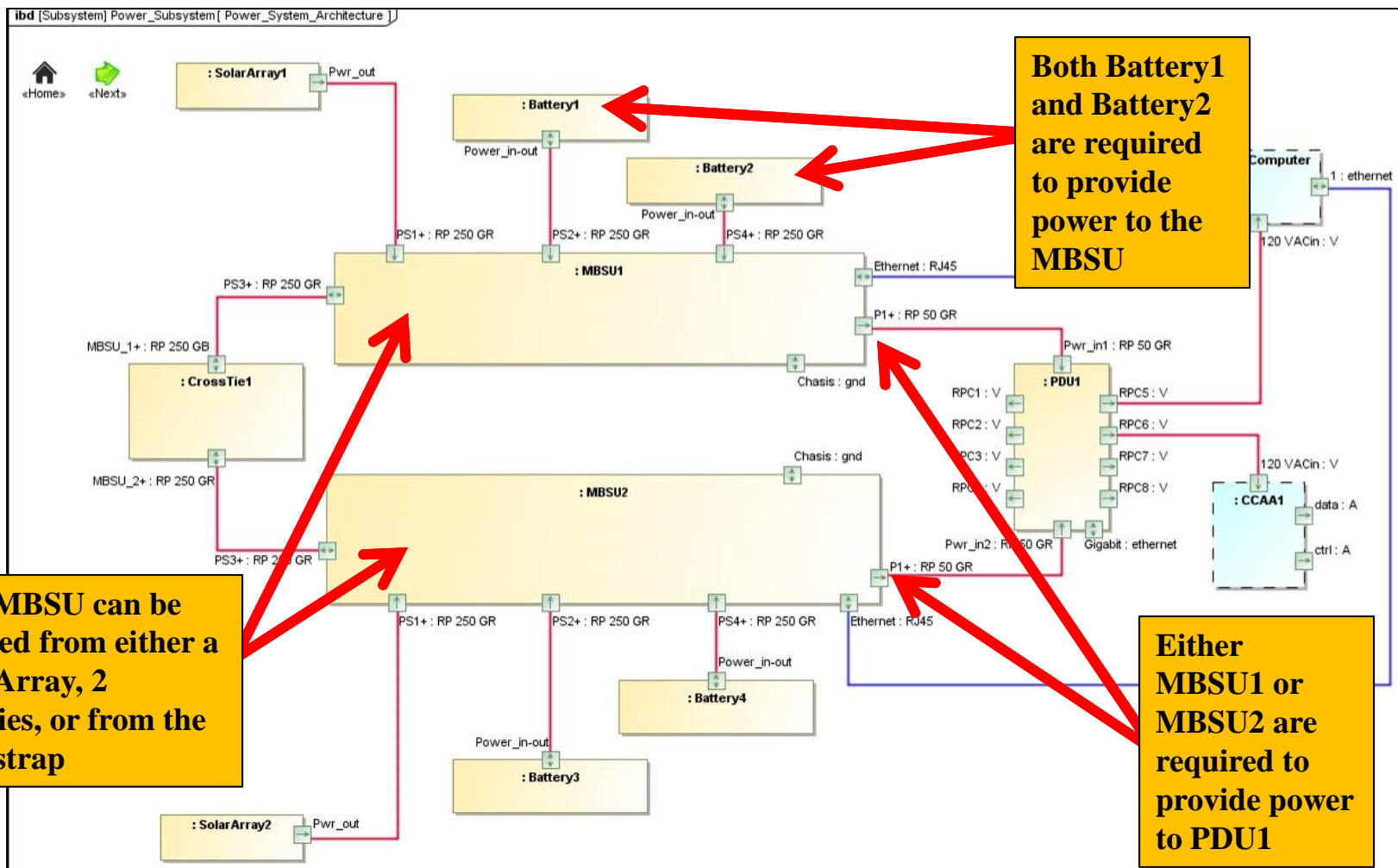


Power Subsystem Internal Block Diagram (IBD)



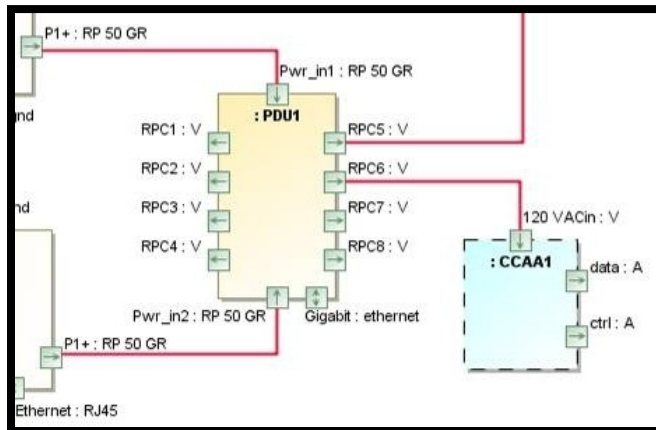
Fan in the Can SysML model

- Demonstrates redundancy in the power system
- Demonstrates power cross-strapping

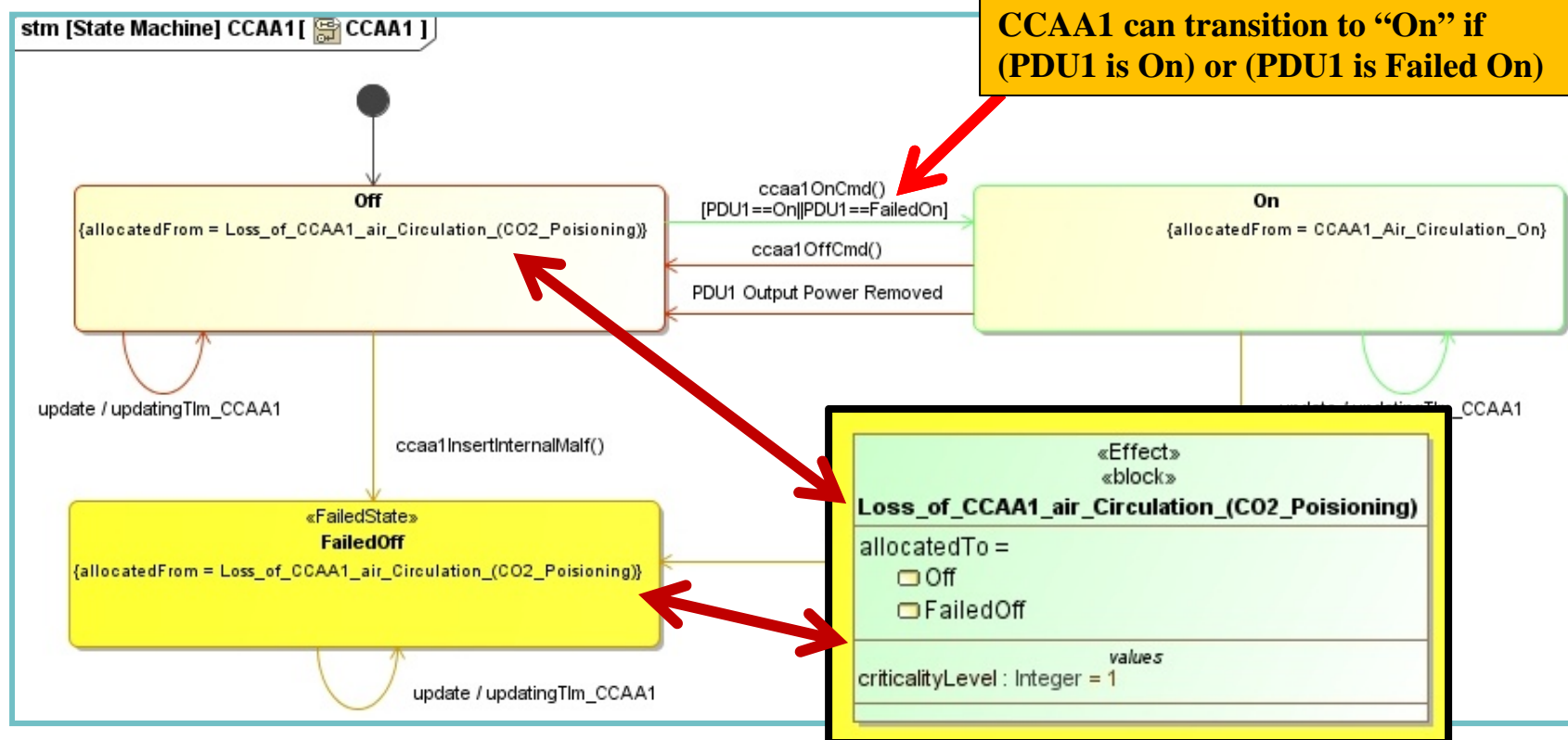




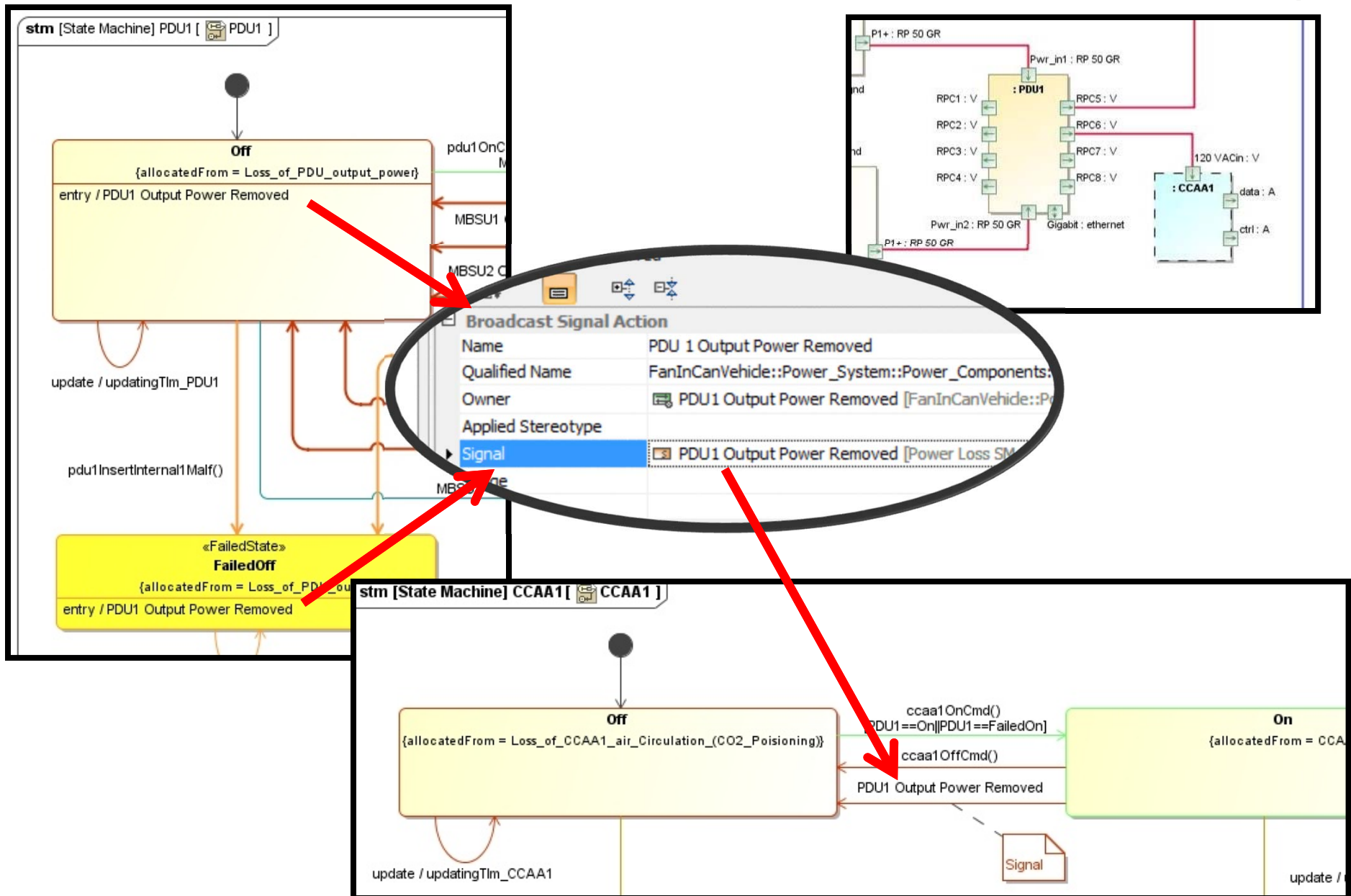
State Machine Diagram for CCAA1



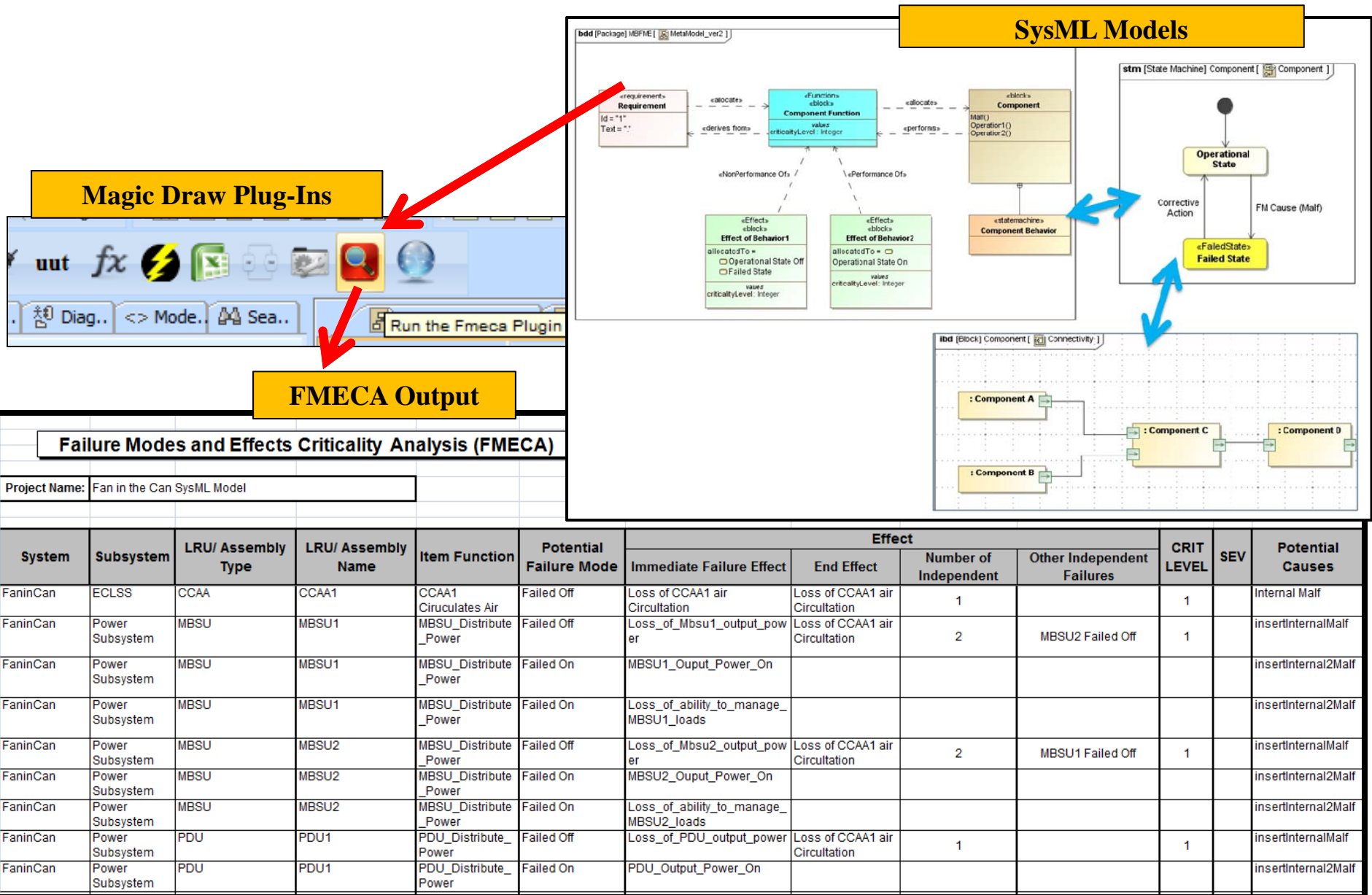
- A Common Cabin Air Assembly (CCAA) function is to provide air circulation
- Loss of the CCAA1's function can result in loss of crew; Assigned a criticality level of 1.



Interactions Between PDU1 and CCAA1



FMECA (Failure Mode and Effects Criticality Analysis) Data Exchange



FMECA Analysis Results



- 10 Failure Modes Can Result in a Critical 1 Level Failure
- Due to redundancy (initial analysis without crosstie):
 - 6 potential failure modes are 2-fault tolerant
 - 2 potential failure modes are 1-fault tolerant
- The failure of the CCAA1 and PDU1 are critical failures requiring reliability measures

Failure Modes and Effects Criticality Analysis (FMECA)

Project Name: Fan in the Can SysML Model

	System	Subsystem	LRU/ Assembly Type	LRU/ Assembly Name	Item Function	Potential Failure Mode	Effect				CRIT LEVEL	SEV	Potential Causes
							Immediate Failure Effect	End Effect	Number of Independent Failures	Other Independent Failures			
9	FanInCan	Power_Subsystem	AMPS_PDU	PDU1	PDU_Distribute_Power	FailedOff	Loss_of_PDU_output_power	Loss_of_CCAA1_air_Circulation_(CO2_Poisoning)	1		1		pdu1InsertInternalMal
10	FanInCan	ECLSS	CCAA	CCAA1	CCAA1_Circulate_Air	FailedOff	Loss_of_CCAA1_air_Circulation_(CO2_Poisoning)	Loss_of_CCAA1_air_Circulation_(CO2_Poisoning)	1		1		ccaa1InsertInternalMal
11	FanInCan	Power_Subsystem	AMPS_MBSU	MBSU1	MBSU_Distribute_Power	FailedOff	Loss_of_MBSU1_output_power	Loss_of_CCAA1_air_Circulation_(CO2_Poisoning)	2	MBSU2 FailedOff	1		mbsu1InsertInternalMal
12	FanInCan	Power_Subsystem	AMPS_MBSU	MBSU2	MBSU_Distribute_Power	FailedOff	Loss_of_MBSU2_output_power	Loss_of_CCAA1_air_Circulation_(CO2_Poisoning)	2	MBSU1 FailedOff	1		mbsu2InsertInternalMal
13	FanInCan	Power_Subsystem	AMPS_Solar_Array	SolarArray1	SA1_Generate_Power,SA_8.1_Generate_Power	FailedOff	Loss_of_SA1_output_power	Loss_of_CCAA1_air_Circulation_(CO2_Poisoning)	3	(Battery1 FailedOff OR Battery2 FailedOff),MBSU2 FailedOff	1		solarArray1InsertInternalMal
14	FanInCan	Power_Subsystem	AMPS_Solar_Array	SolarArray2	SA2_Generate_Power,SA_8.1_Generate_Power	FailedOff	Loss_of_SA2_output_power	Loss_of_CCAA1_air_Circulation_(CO2_Poisoning)	3	(Battery3 FailedOff OR Battery4 FailedOff),MBSU1 FailedOff	1		solarArray2InsertInternalMal
15	FanInCan	Power_Subsystem	AMPS_Modular_Lithium_Battery	Battery1	Battery_Generate_Power	FailedOff	Loss_of_Battery1_output_power	Loss_of_CCAA1_air_Circulation_(CO2_Poisoning)	3	SolarArray1 FailedOff,MBSU2 FailedOff	1		battery1InsertInternalMal
16	FanInCan	Power_Subsystem	AMPS_Modular_Lithium_Battery	Battery2	Battery_Generate_Power	FailedOff	Loss_of_Battery2_output_power	Loss_of_CCAA1_air_Circulation_(CO2_Poisoning)	3	SolarArray1 FailedOff,MBSU2 FailedOff	1		battery2InsertInternalMal
17	FanInCan	Power_Subsystem	AMPS_Modular_Lithium_Battery	Battery3	Battery_Generate_Power	FailedOff	Loss_of_Battery3_output_power	Loss_of_CCAA1_air_Circulation_(CO2_Poisoning)	3	SolarArray2 FailedOff,MBSU1 FailedOff	1		battery3InsertInternalMal
18	FanInCan	Power_Subsystem	AMPS_Modular_Lithium_Battery	Battery4	Battery_Generate_Power	FailedOff	Loss_of_Battery4_output_power	Loss_of_CCAA1_air_Circulation_(CO2_Poisoning)	3	SolarArray2 FailedOff,MBSU1 FailedOff	1		battery4InsertInternalMal
19	FanInCan	Power_Subsystem	AMPS_MBSU	MBSU1	MBSU_Distribute_Power	FailedOn	Loss_of_ability_to_manage_MBSU1_loads						mbsu1InsertInternalMal
20	FanInCan	Power_Subsystem	AMPS_MBSU	MBSU1	MBSU_Distribute_Power	FailedOn	MBSU1_Output_Power_On						mbsu1InsertInternalMal
21	FanInCan	Power_Subsystem	AMPS_MBSU	MBSU2	MBSU_Distribute_Power	FailedOn	Loss_of_ability_to_manage_MBSU2_loads						mbsu2InsertInternalMal
22	FanInCan	Power_Subsystem	AMPS_MBSU	MBSU2	MBSU_Distribute_Power	FailedOn	MBSU2_Output_Power_On						mbsu2InsertInternalMal
23	FanInCan	Power_Subsystem	AMPS_PDU	PDU1	PDU_Distribute	FailedOn	PDU Output Power On						pdu1InsertInternalMal

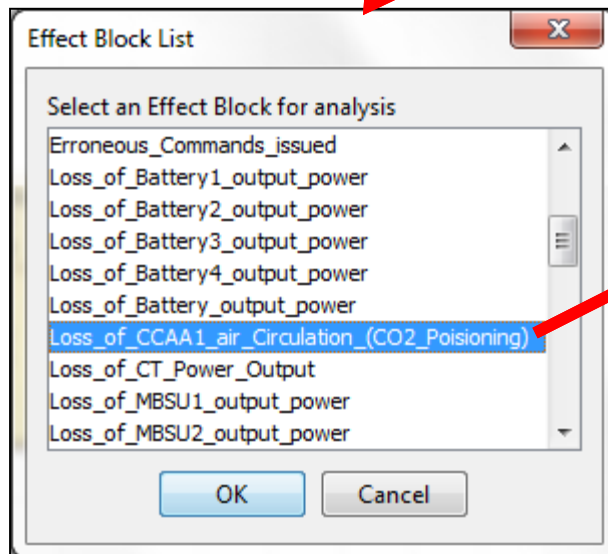
FTA (Fault Tree Analysis) Data Exchange



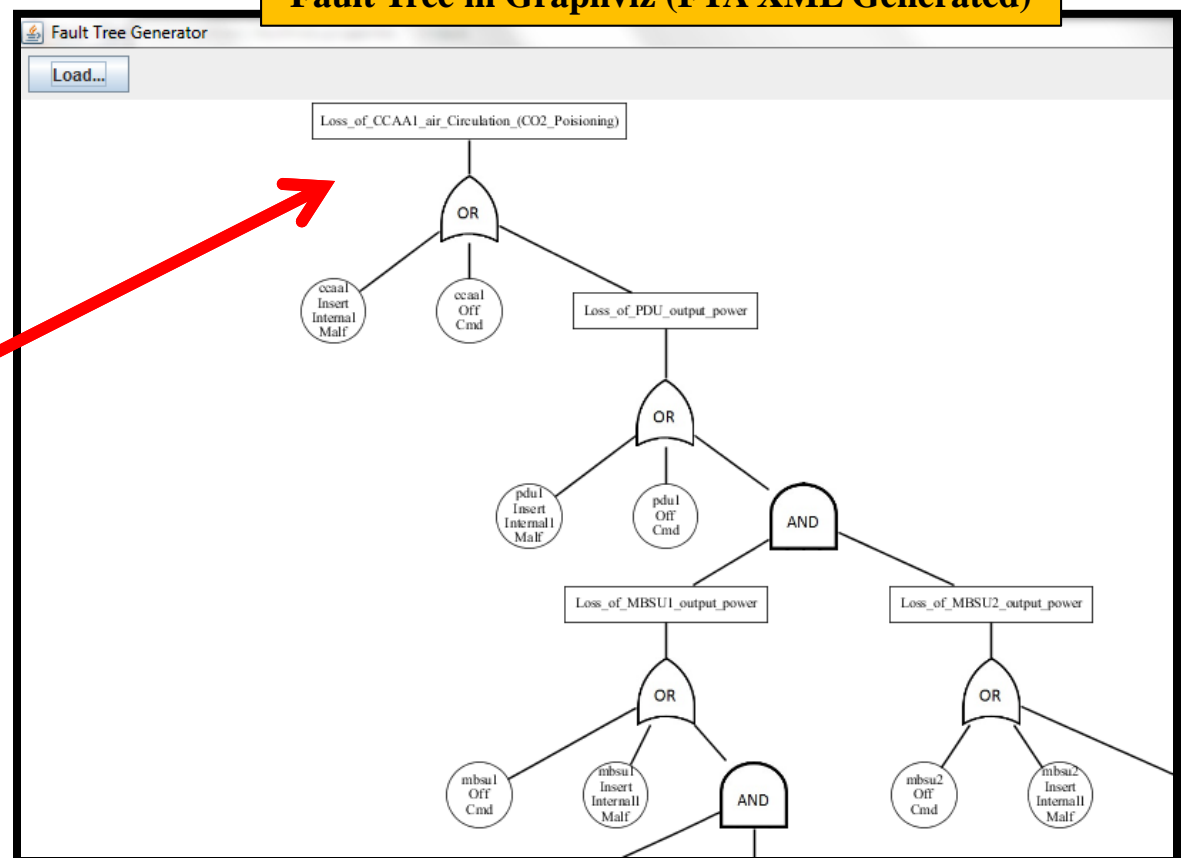
Magic Draw Plug-Ins



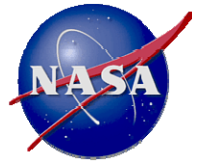
Select Top Level Event to Analyze



Fault Tree in Graphviz (FTA XML Generated)



Future Directions / Conclusions

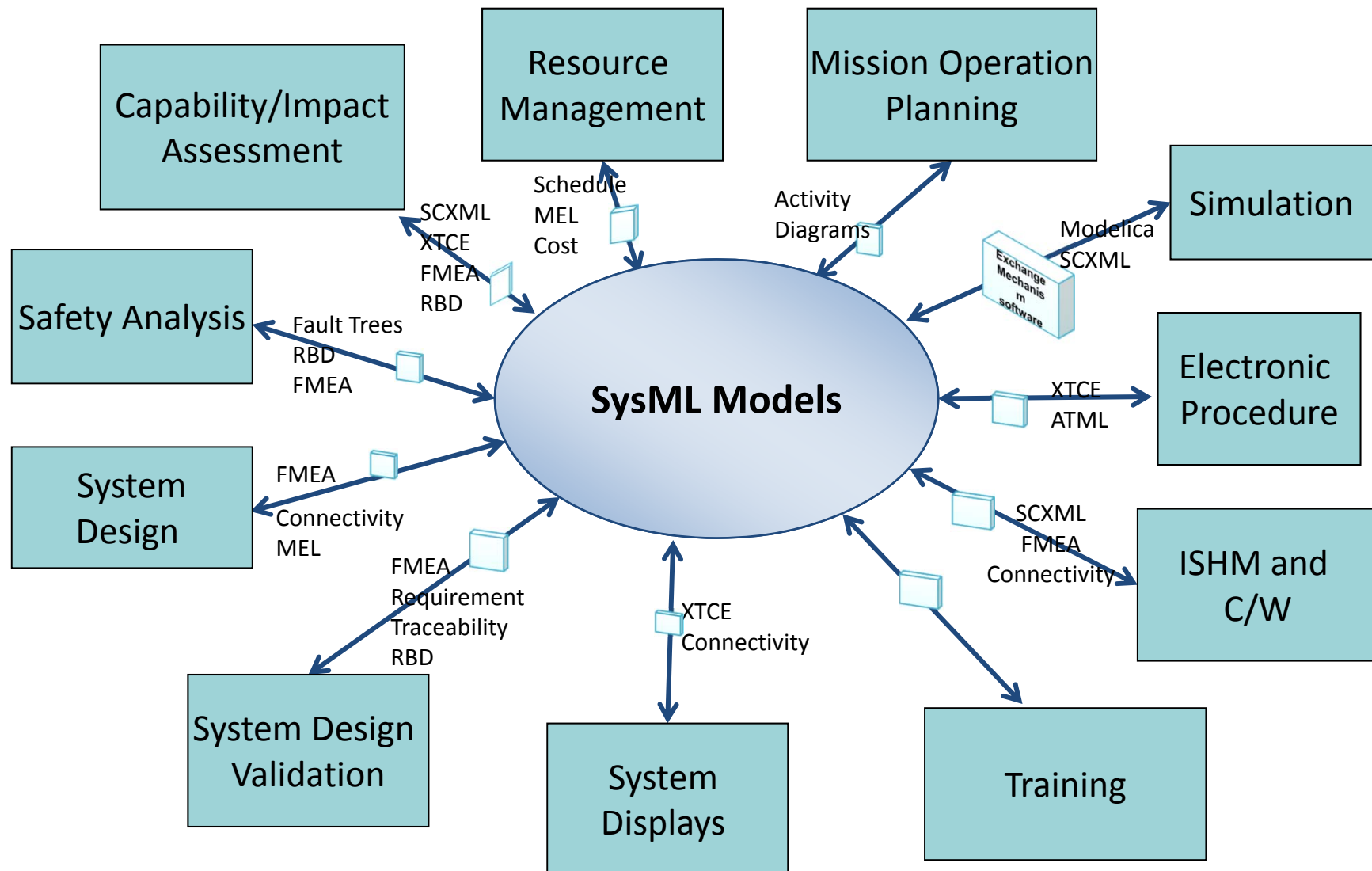


- ◆ **Expand the FM meta-models (model attributes) to support additional FM products**
- ◆ **Continue collaboration with additional FM analysis experts (e.g., QSI TEAMS)**
- ◆ **Demonstrate the tools on NASA systems of varying complexity (e.g., CDS 2.0)**
- ◆ **Support automated generation of simulations with failure injection**



Uses of System Models

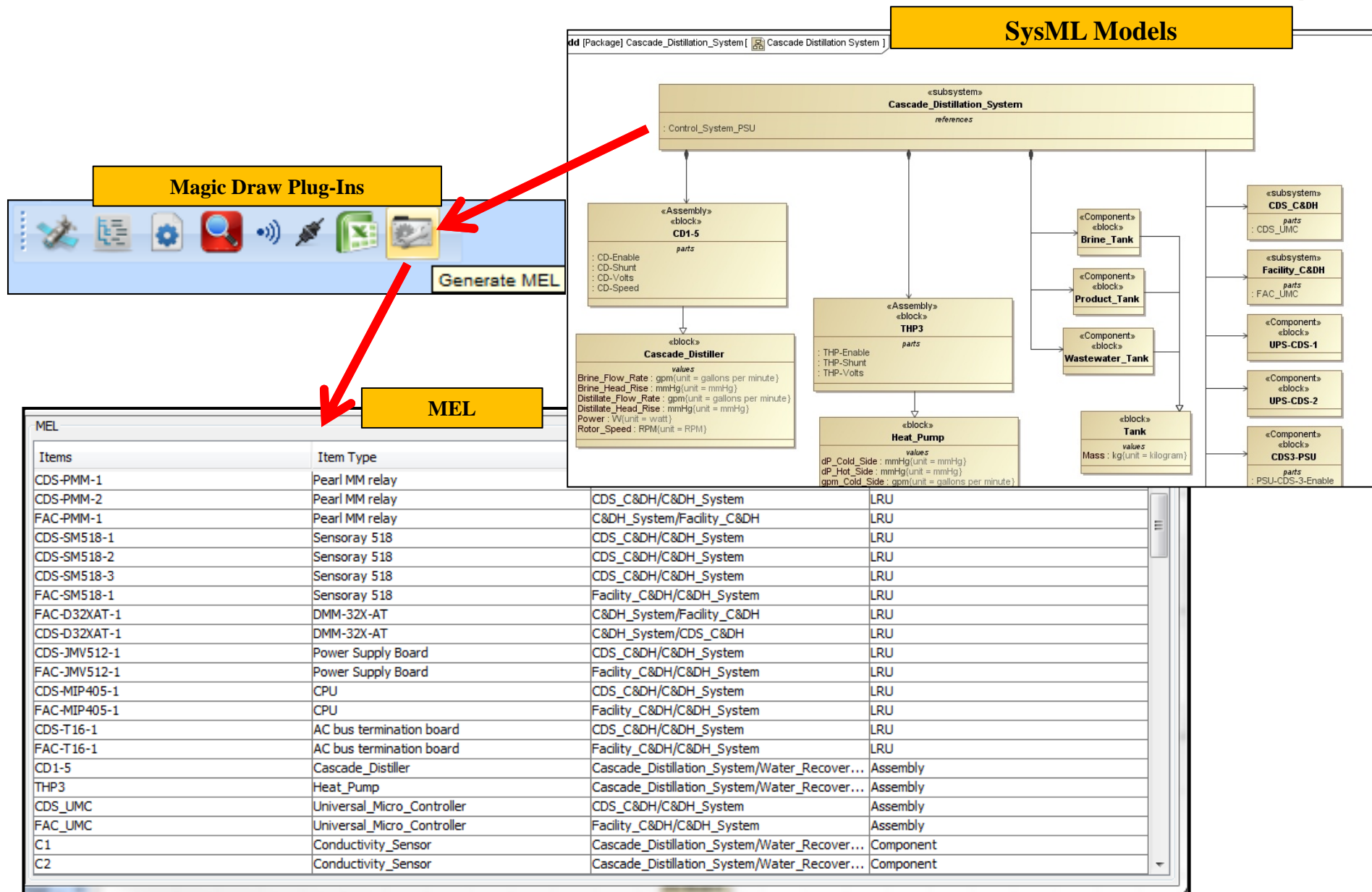
Model once and Use many times



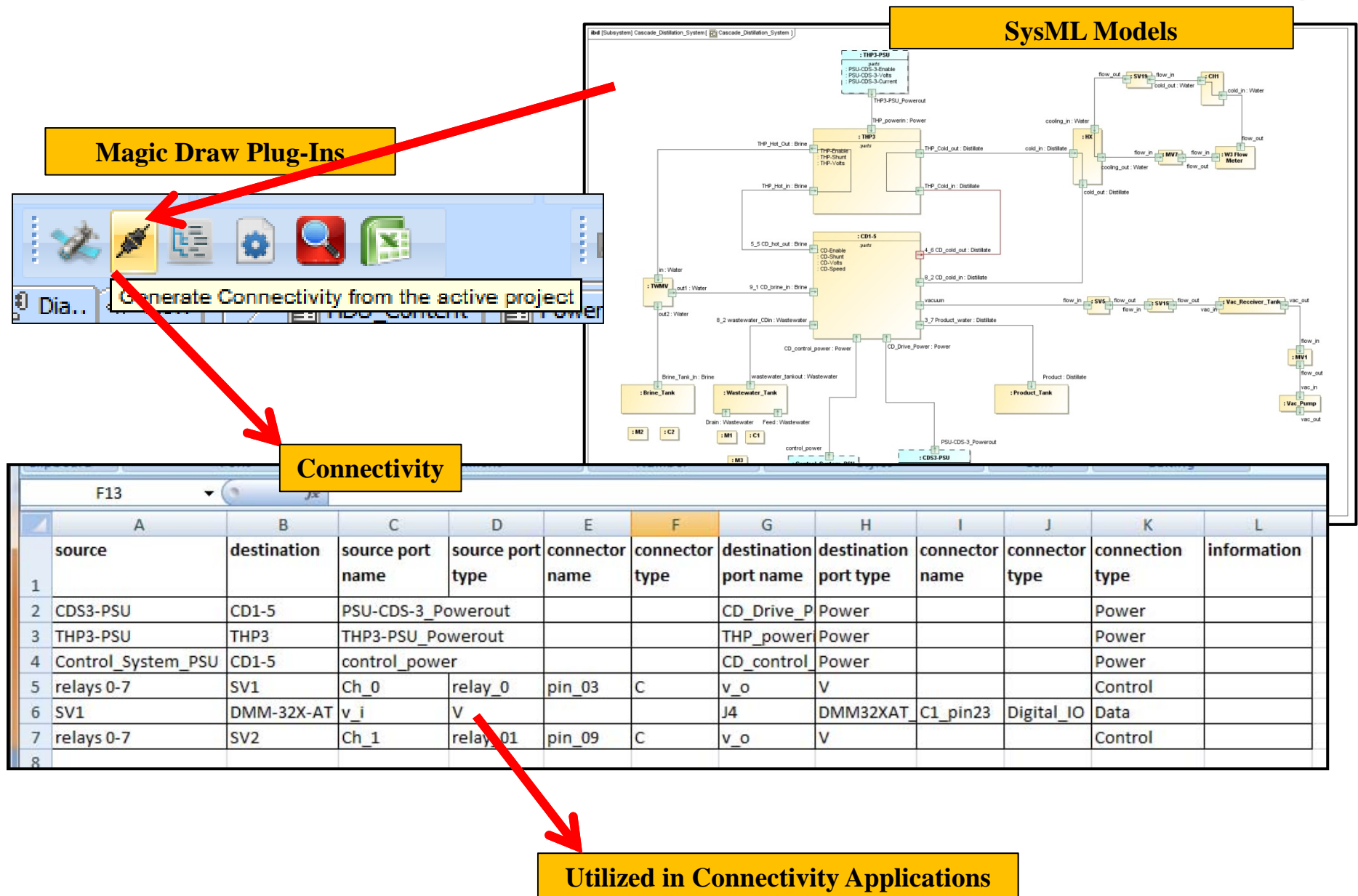
Backup Slides



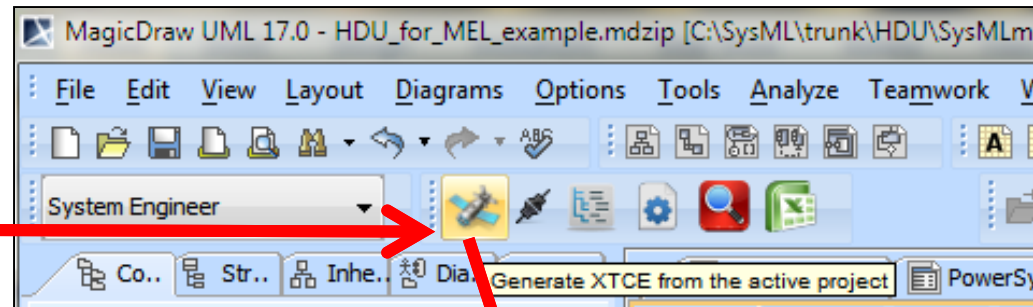
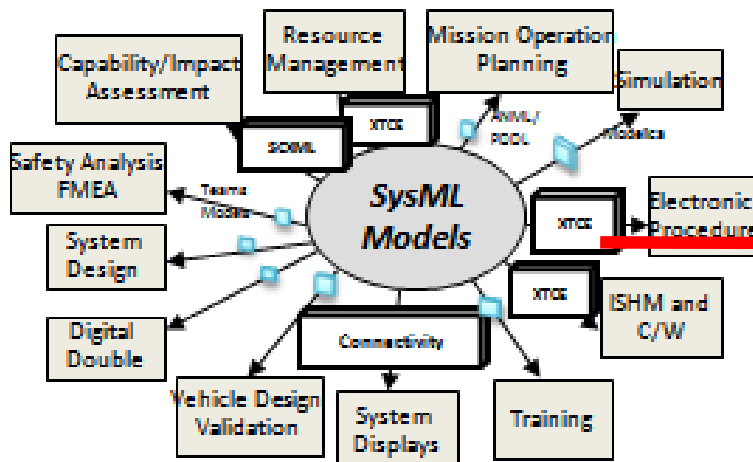
Generate MEL from SysML



Connectivity Data Exchange

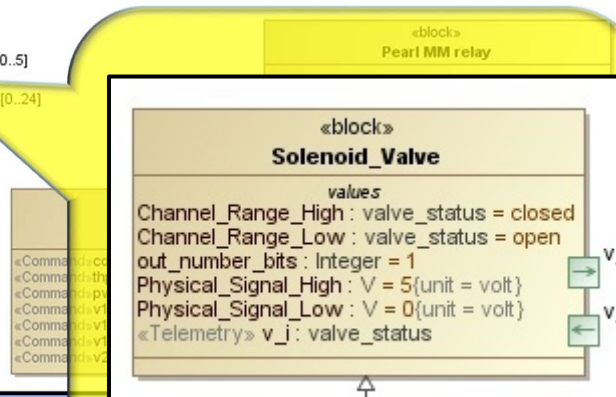
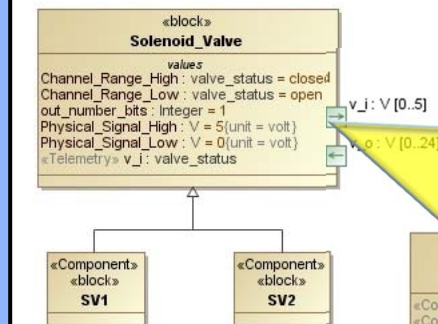


XTCE Exchange

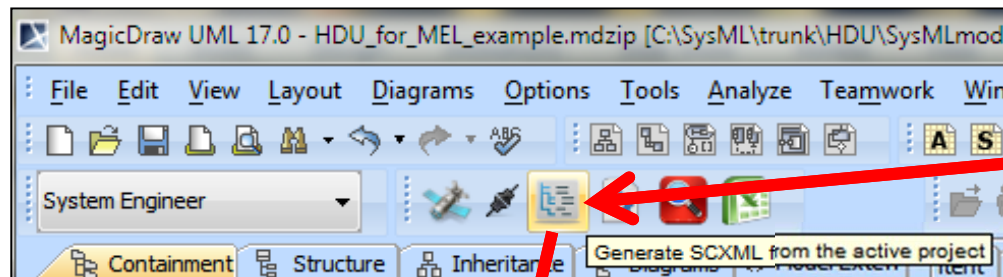
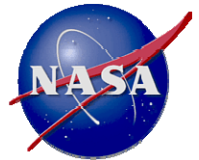


XML Telemetric and Command Exchange (XTCE) : OMG standard for Spacecraft T&C

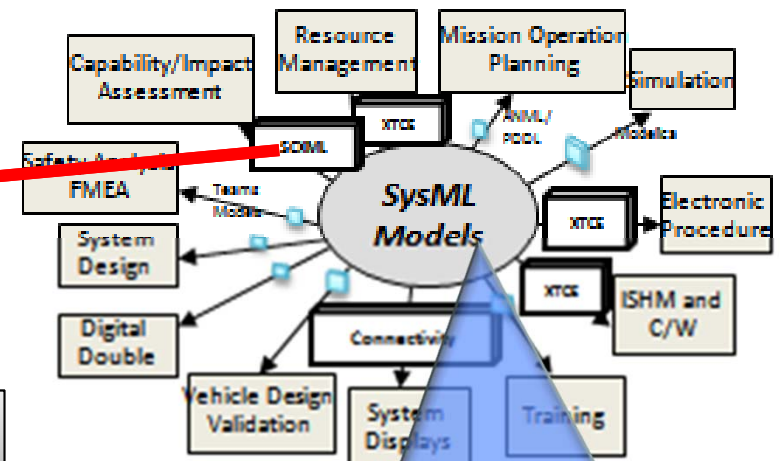
```
<SpaceSystem name="RIU2">
  <AliasSet>
    <Alias alias="02" nameSpace="id"/>
    <Alias alias="020602" nameSpace="interface"/>
  </AliasSet>
  <Header classification="INTERFACE"/>
  <TelemetryMetaData>
    <ParameterSet>
      <Parameter
        parameterTypeRef="HUMIDITY_DEWPOINT_SENSOR"
        shortDescription="GEOLAB_GB_HUMIDITY1_DEWPOINT_SE
        NSOR" name="020602018001">
        <ParameterProperties dataSource="telemetry">
        </ParameterProperties>
      </Parameter>
      <Parameter parameterTypeRef="VALIDITY"
        name="020602054001">
        <ParameterProperties dataSource="telemetry">
        </ParameterProperties>
      </Parameter>
    </ParameterSet>
  </TelemetryMetaData>
  <SystemName>CORE.GEOLAB.RIU2.HUMIDITY_DEWPOINT_
  SENSOR.1</SystemName>
  <SystemName>CORE.GEOLAB.RIU2.VALIDITY.1</SystemName>
</SpaceSystem>
```



State Machine (SCXML)/FSM Exchange



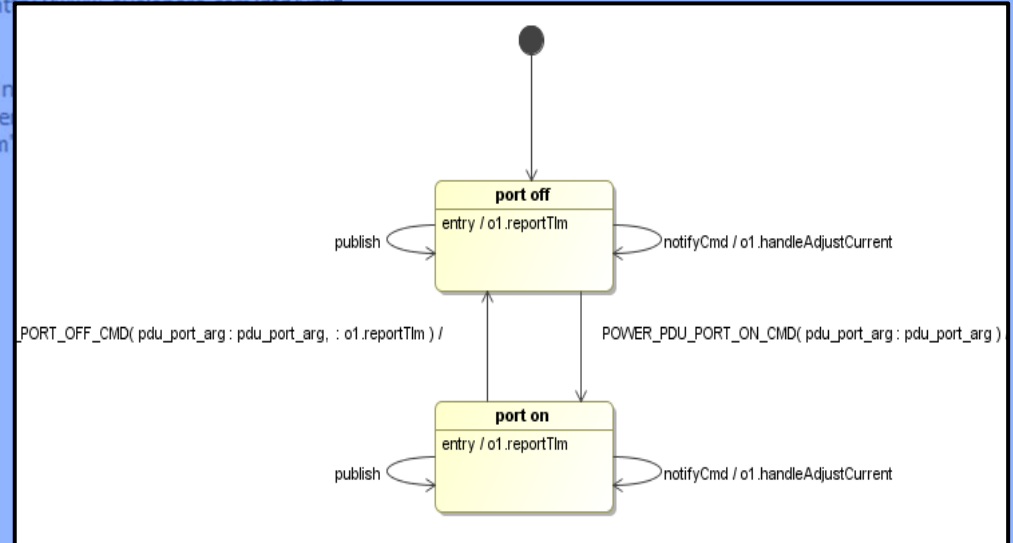
SCXML: "State Chart extensible Markup Language". Provides a generic state-machine based execution environment based on Harel State Tables.



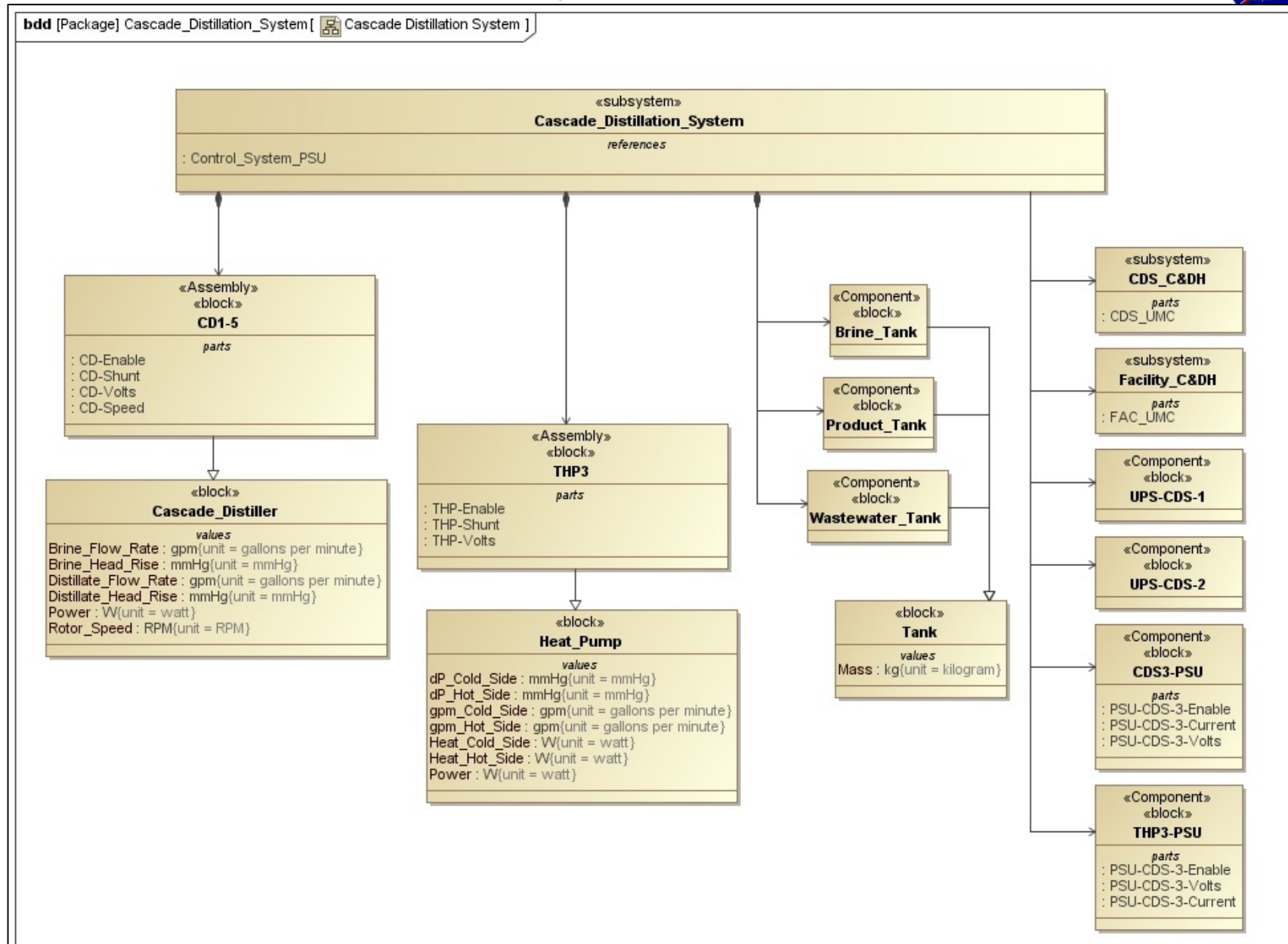
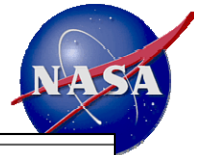
C:\SysML\trunk\HDU\SysMLmodels\PowerSystem.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE model PUBLIC "-//evelopers Corp./DTD State machine model V1.0//EN" "http://www.evelopers.com/DTD/StateMachineModelV1.0.dtd">
<model name="Data">
  <controlledObject class="com.tietronix.controllers.PowerSystemInterfaceController">
    <eventProvider class="com.evelopers.unimod.adapter.standalone.provider.ScriptEventProvider">
      <association clientRole="p1" supplierRole="PowerSystem" targetRef="PowerSystem">
      </association>
    </eventProvider>
    <rootStateMachine>
      <stateMachineRef name="PowerSystem"/>
    </rootStateMachine>
    <stateMachine name="PowerSystem">
      <state name="TOP" type="NORMAL">
        <state name="s1" type="INITIAL"/>
        <state name="Running" type="NORMAL">
          <stateMachineRef name="pdu"/>
          <stateMachineRef name="rpc"/>
        </state>
      </state>
      <transition name="" sourceRef="s1" targetRef="Running"/>
    </stateMachine>
    <stateMachine name="bank1">
      <association clientRole="bank1" supplierRole="o1" targetRef="o1"/>
      <state name="TOP" type="NORMAL">

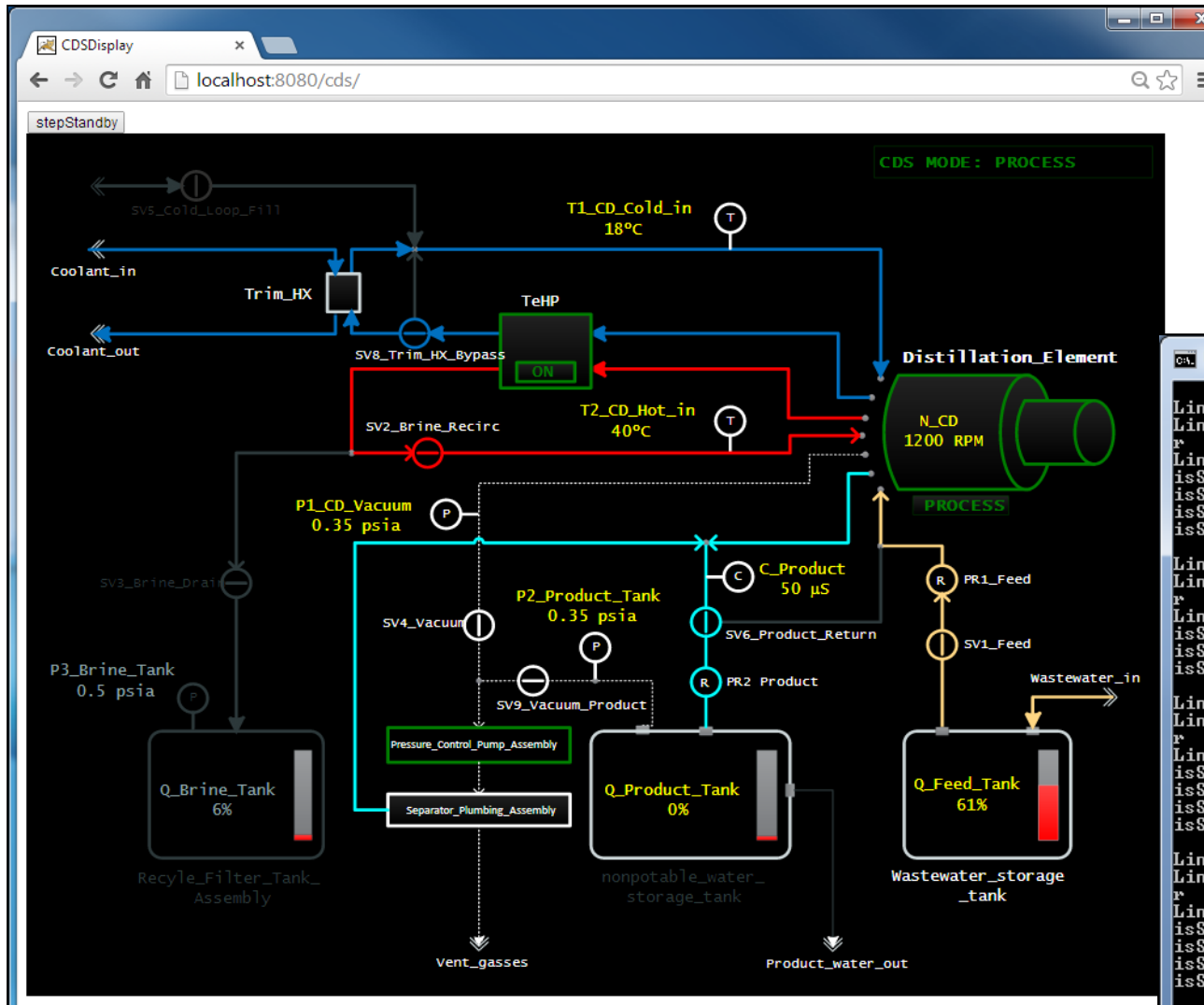
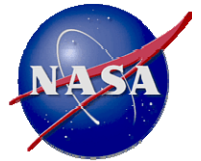
```



CDS System Model



Concept of Operations



Unimod Simulator ConOps Standby to Steady State

```
Line 39 (comment) // Step 2b
Line:40 Script Paused. Press 'r' to resume!
r
Line:40 Script Resumed.
isStateMachineInStateWithHeirarchy currentState:
isStateMachineInStateWithHeirarchy currentState:
isStateMachineInStateWithHeirarchy currentState:
isStateMachineInStateWithHeirarchy currentState:

Line 46 (comment) // Step 3a
Line:47 Script Paused. Press 'r' to resume!
r
Line:47 Script Resumed.
isStateMachineInStateWithHeirarchy currentState:
isStateMachineInStateWithHeirarchy currentState:
isStateMachineInStateWithHeirarchy currentState:

Line 52 (comment) // Step 3b
Line:53 Script Paused. Press 'r' to resume!
r
Line:53 Script Resumed.
isStateMachineInStateWithHeirarchy currentState:
isStateMachineInStateWithHeirarchy currentState:
isStateMachineInStateWithHeirarchy currentState:

Line 59 (comment) // Step 4a
Line:60 Script Paused. Press 'r' to resume!
r
Line:60 Script Resumed.
isStateMachineInStateWithHeirarchy currentState:
isStateMachineInStateWithHeirarchy currentState:
isStateMachineInStateWithHeirarchy currentState:
isStateMachineInStateWithHeirarchy currentState:

Line 66 (comment) // Step 5
Line:67 Script Paused. Press 'r' to resume!
```